(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－32267
（Ｐ２００２－３２２６７Ａ）
(43)公開日　平成14年１月31日(2002.1.31)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
G06F 12/14	310	G06F 12/14	310	B 5B017
G11C 16/02		G11C 17/00	601	P 5B025
H01L 27/04		H01L 27/04		U 5F038
21/822				

審査請求　有　請求項の数３　ＯＬ　（全５頁）

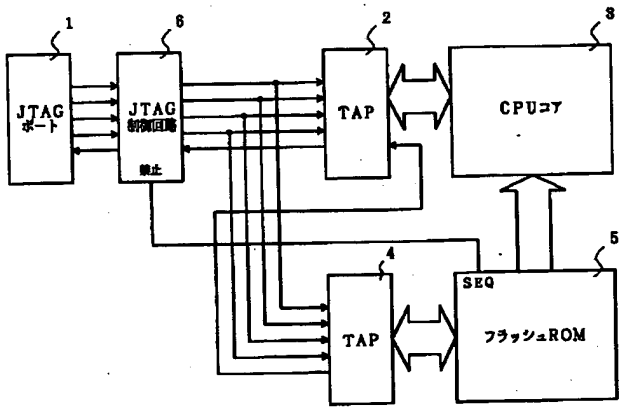
(21)出願番号　特願2000－216983(Ｐ2000－216983)
(22)出願日　平成12年７月18日(2000.7.18)

(71)出願人　591049893
株式会社　沖マイクロデザイン
宮崎県宮崎郡清武町大字木原7083番地
(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　新森　信明
宮崎県宮崎郡清武町大字木原7083番地　株式会社沖マイクロデザイン内
(74)代理人　100089635
弁理士　清水　守　（外２名）

Ｆターム(参考)　5B017 AA03 BA04 BA09 BB09 CA12
5B025 AD14 AE10
5F038 BH01 BH20 DF11 EZ20

(54)【発明の名称】半導体回路

(57)【要約】
【課題】　フラッシュＲＯＭの内容が第三者に読み出されることを防止することができる半導体回路を提供する。
【解決手段】　半導体回路において、フラッシュＲＯＭ５のセキュリティビットに“１”を書込むと、ＪＴＡＧポート１を使用したフラッシュＲＯＭライタによる読出しだけでなく、ＪＴＡＧポート１を使用したデバッグ機能も使用不可能となるため、フラッシュＲＯＭ５の内容が第三者に読出されることが全く無くなる。



1

【特許請求の範囲】

【請求項１】　ＪＴＡＧポートとＴＡＰの間にフラッシュＲＯＭのセキュリティビットで制御されるＪＴＡＧ制御回路を具備することを特徴とする半導体回路。

【請求項２】　フラッシュＲＯＭのセキュリティビットとＪＴＡＧ制御回路の間にインヒビットＮＡＮＤゲートとマイコン汎用ポートをＰｉｎスクランブル回路にてデコードする回路を設け、前記Ｐｉｎスクランブル回路の出力の逆相を前記インヒビットＮＡＮＤゲートの片方に入力し、前記フラッシュＲＯＭのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする半導体回路。

【請求項３】　フラッシュＲＯＭのセキュリティビットとＪＴＡＧ制御回路の間にインヒビットＮＡＮＤゲートとマイコン内部レジスタとしてデバッグイネーブルレジスタを設け、前記インヒビットＮＡＮＤゲートに前記デバッグイネーブルレジスタの出力の逆相を入力し、前記フラッシュＲＯＭのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする半導体回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、半導体回路に関するものである。

【０００２】

【従来の技術】図４はかかる従来の半導体回路としてのＪＴＡＧ回路の構成図である。

【０００３】この図において、１はＪＴＡＧ（Ｊｏｉｎｔ　Ｔｅｓｔ　Ａｃｔｉｏｎ　Ｇｒｏｕｐ）ポート、２，４はＴＡＰ（Ｔｅｓｔ　Ａｃｃｅｓｓ　Ｐｏｒｔ）、３はＣＰＵコア、５はフラッシュ（Ｆｌａｓｈ）ＲＯＭである。

【０００４】昨今のマイコン（マイクロコントローラ）では、ＪＴＡＧ等を使用したデバッグ機能が搭載されているマイコンが主流になってきている。このデバッグ機能を使用してマイコンのソフト開発者はアプリケーションソフトのデバッグを行い、容易にプログラムを開発できるようになっている。

【０００５】また、最近多くなっているフラッシュＲＯＭ内蔵マイコンでは、ＪＴＡＧを使用してフラッシュＲＯＭの書換えが実行できるようになっている。そして、このフラッシュＲＯＭにはセキュリティビットを設け、フラッシュＲＯＭの内容が第三者に読み出せないようになっている。因みに、フラッシュＲＯＭに書き込まれるデータは、ユーザー作成のアプリケーションプログラムであり、上記したセキュリティビットをセットすると、フラッシュＲＯＭのライタでの読み出し及び部分的な領域の書換えが不可能になる（例えば、特開平１１－８５６２０号公報参照）。

【０００６】

2

【発明が解決しようとする課題】しかしながら、上記した従来のフラッシュＲＯＭのセキュリティはセキュリティビットに“１”をセット後はＪＴＡＧを使用したフラッシュＲＯＭライタではフラッシュＲＯＭの内容が読み出されないようになってはいるが、ＪＴＡＧを使用したデバッグ機能では、図４に示すように、ＪＴＡＧインターフェースとしてのＪＴＡＧポート１のＴＡＰ２にてＣＰＵコア３に対し直接命令を挿入できるため、フラッシュＲＯＭ５の内容を容易にダウンロードできる。このためセキュリティビットの意味をなしていない。

【０００７】本発明は、上記問題点を除去し、フラッシュＲＯＭの内容が第三者に読出されることを防止することができる半導体回路を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明は、上記目的を達成するために、

〔１〕半導体回路において、ＪＴＡＧポートとＴＡＰの間にフラッシュＲＯＭのセキュリティビットで制御されるＪＴＡＧ制御回路を具備することを特徴とする。

【０００９】〔２〕半導体回路において、フラッシュＲＯＭのセキュリティビットとＪＴＡＧ制御回路の間にインヒビットＮＡＮＤゲートとマイコン汎用ポートをＰｉｎスクランブル回路にてデコードする回路を設け、前記Ｐｉｎスクランブル回路の出力の逆相を前記インヒビットＮＡＮＤゲートの片方に入力し、前記フラッシュＲＯＭのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする。

【００１０】〔３〕半導体回路において、フラッシュＲＯＭのセキュリティビットとＪＴＡＧ制御回路の間にインヒビットＮＡＮＤゲートとマイコン内部レジスタとしてデバッグイネーブルレジスタを設け、前記インヒビットＮＡＮＤゲートに前記デバッグイネーブルレジスタの出力の逆相を入力し、前記フラッシュＲＯＭのセキュリティビットの出力をもう片方に入力した回路を具備することを特徴とする。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態について詳細に説明する。

【００１２】まず、本発明の第１実施について説明する。

【００１３】図１は本発明の第１実施例を示す半導体回路の回路図である。

【００１４】この実施例では、ＪＴＡＧポート１とＴＡＰ２，４の間に、信号を禁止したり許可したりすることのできるＪＴＡＧ制御回路６を設け、この制御をフラッシュＲＯＭ５のセキュリティビットで行うように構成したものである。なお、図１において、３はＣＰＵ（中央処理装置）である。

【００１５】以下、この実施例の回路の動作について説明する。

【００１６】プログラマーはＪＴＡＧポート１を使用してデバッグを行いプログラムの開発を行うが、プログラムの開発が終了すると、フラッシュＲＯＭ５のセキュリティビット（ＳＥＱ）に“１”を書込む。セキュリティビットが“１”になるとＪＴＡＧ制御回路６に禁止信号として入力され、ＪＴＡＧポート１とＴＡＰ２，４間の信号のやり取りが禁止され、結果としてＪＴＡＧポート１を使用したデバッグが使用できなくなる。つまり、ＪＴＡＧポート１とＴＡＰ２，４の間にＯＲゲート（論理を変えればＡＮＤゲートでも可能）を挿入し、ＳＥＱ＝１となったら、ＴＡＰ２，４には“１”しか入力されなくなるような回路構成にする。

【００１７】このように第１実施例によれば、フラッシュＲＯＭ５のセキュリティビットに“１”を書込むとＪＴＡＧポート１を使用したフラッシュＲＯＭライタによる読出しだけでなく、ＪＴＡＧポート１を使用したデバッグ機能も使用不可能となるため、フラッシュＲＯＭ５の内容が第三者に読出されることが全く無くなる。

【００１８】次に、本発明の第２実施例について説明する。

【００１９】図２は本発明の第２実施例を示す半導体回路の回路図である。なお、第１実施例と同じ部分には同じ符号を付してその説明は省略する。

【００２０】この実施例ではフラッシュＲＯＭ５とＪＴＡＧ制御回路６のＪＴＡＧ制御ポートとの間にインヒビット（ＩＮＨＩＢＩＴ）ＮＡＮＤゲート７を設け、且つマイコンの汎用ポート９をデコードするＰｉｎスクランブル回路８を設けるようにしたものである。なお、Ｐｉｎスクランブル回路８は汎用ポート９のうち１本または数本をデコードし、インヒビットＮＡＮＤゲート７に入力するもので、チップ毎にマスクオプション等で指定できるものである。

【００２１】以下、この実施例の回路の動作について説明する。

【００２２】上記した第１実施例と同様にプログラマーはデバッグ終了後にフラッシュＲＯＭ５のセキュリティビットに“１”を書込み、第三者がＪＴＡＧポート１を使用したデバッグ機能によるフラッシュＲＯＭ５の内容の読出しを禁止する。しかし、セキュリティ書込み後でもチップ毎に設定されたＰｉｎスクランブル回路８で汎用ポート９をデコードすることにより、ＪＴＡＧポート１でのデバッグが可能となる。

【００２３】このように第２実施例によれば、フラッシュＲＯＭ５のセキュリティビット書込み後もチップ毎に設定されたＰｉｎスクランブル回路８の内容（マスクオプション等の内容）を知っているプログラマーはＪＴＡＧポート１を使用してデバッグが行えるため、セキュリティ書換え後の動作不具合や市場クレーム品等の解析が容易になる。また、Ｐｉｎスクランブル回路８を知らない第三者にはＪＴＡＧポート１を使用したデバッグは使用できないため、フラッシュＲＯＭ５の内容が第三者に漏れることはない。

【００２４】次に、本発明の第３実施例について説明する。

【００２５】図３は本発明の第３実施例を示す半導体回路の回路図である。なお、第１実施例と同じ部分には、同じ符号を付してそれらの説明は省略する。

【００２６】この実施例ではフラッシュＲＯＭ５のセキュリティビットとＪＴＡＧ制御回路６との間のインヒビットＮＡＮＤゲート７の一つに入力されるデバッグイネーブル（ＤＢＧ＿ＥＮ）レジスタ１０というマイコンの内部レジスタを設けるようにしたものである。

【００２７】以下、この実施例の回路の動作について説明する。

【００２８】上記した第１及び第２実施例と同様に、プログラマーはデバッグ終了後はフラッシュＲＯＭ５のセキュリティビットに“１”を書込み、第三者によるフラッシュＲＯＭ５の内容の読出しを禁止する。しかし、プログラムの一部にレジスタに“１”をセットするプログラムを用意しておき、必要に応じてそのプログラムを起動し、デバッグイネーブルレジスタ１０を“１”にセットすることにより、ＪＴＡＧポート１でのデバッグが可能となる。

【００２９】このように第３実施例によれば、第２実施例と同様に、フラッシュＲＯＭ５のセキュリティビット書込み後もデバッグイネーブルレジスタ１０のセットのプログラムを起動することにより、ＪＴＡＧポート１でのデバッグが可能となる。また、第２実施例と異なりプログラム的に制御するのでマスクオプション等の無駄な費用が発生しない。更に、当然デバッグイネーブルレジスタ１０のセットのプログラムの起動はフラッシュＲＯＭ５のプログラムの内容を理解しているプログラム開発者のみが実行できるもので、プログラムの内容を知らない第三者がデバッグイネーブルレジスタ１０をセットすることはできない。

【００３０】したがって、フラッシュＲＯＭ５のセキュリティビット書込み後のデバッグが容易に行え、且つ第三者がフラッシュＲＯＭ５の内容をＪＴＡＧポート１でのデバッグ機能を使用して読み出すことを防止することができる。

【００３１】なお、本発明は上記実施例に限定されるものではなく、本発明の趣旨に基づいて種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【００３２】

【発明の効果】以上、詳細に説明したように、本発明によれば、次のような効果を奏することができる。

（１）フラッシュＲＯＭのセキュリティビットに“１”を書込むとＪＴＡＧポートを使用したフラッシュＲＯＭライタによる読出しだけでなく、ＪＴＡＧポートを使用

したデバッグ機能も使用不可能となるため、フラッシュＲＯＭの内容が第三者に読み出されることが全く無くなる。

（２）フラッシュＲＯＭのセキュリティビット書込み後もチップ毎に設定されたＰｉｎスクランブル回路の内容（マスクオプション等の内容）を知っているプログラマーはＪＴＡＧポートを使用してデバッグが行えるため、セキュリティ書換え後の動作不具合や市場クレーム品等の解析が容易になる。また、Ｐｉｎスクランブルを知らない第三者にはＪＴＡＧポートを使用したデバッグは使用できないためフラッシュＲＯＭの内容が第三者に漏れることはない。

（３）上記（２）と同様にフラッシュＲＯＭのセキュリティビット書込み後もデバッグイネーブルレジスタのセットのプログラムを起動することにより、ＪＴＡＧポートでのデバッグが可能となる。また、上記（２）と異なりプログラム的に制御するものでマスクオプション等の無駄な費用が発生しない。また、当然デバッグイネーブルレジスタのセットのプログラムの起動はフラッシュＲＯＭのプログラムの内容を理解しているプログラム開発者のみが実行できるものでプログラムの内容を知らない第三者がデバッグイネーブルレジスタをセットすることはできない。したがって、フラッシュＲＯＭのセキュリティビット書込み後のデバッグが容易に行え、且つ第三者がフラッシュＲＯＭの内容をＪＴＡＧポートでのデバッグ機能を使用して読み出すことを防止することができる。

【図面の簡単な説明】

【図１】本発明の第１実施例を示す半導体回路の回路図である。

【図２】本発明の第２実施例を示す半導体回路の回路図である。

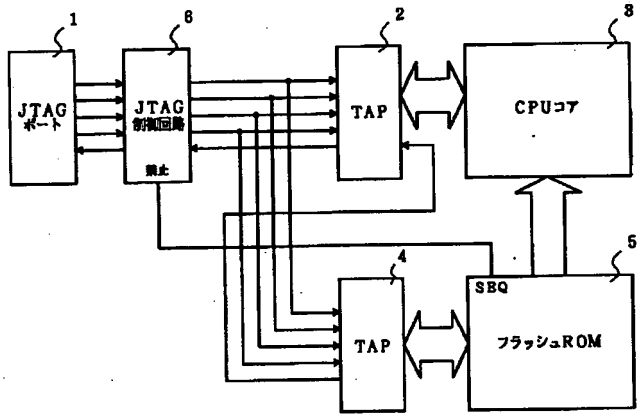
【図３】本発明の第３実施例を示す半導体回路の回路図である。

【図４】従来の半導体回路としてのＪＴＡＧ回路の構成図である。

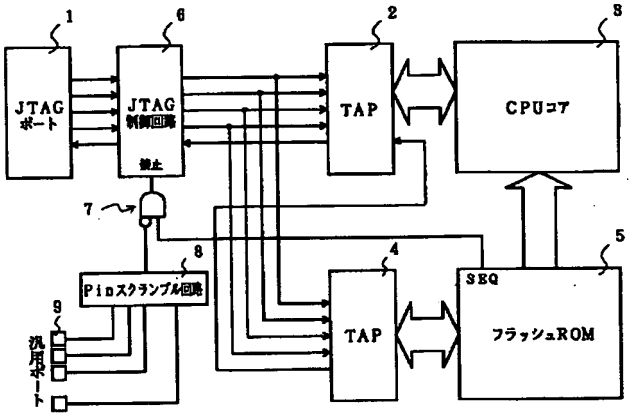
【符号の説明】

１　　ＪＴＡＧポート
２，４　　ＴＡＰ
３　　ＣＰＵコア
５　　フラッシュＲＯＭ
６　　ＪＴＡＧ制御回路
７　　インヒビット（ＩＮＨＩＢＩＴ）ＮＡＮＤゲート
８　　Ｐｉｎスクランブル回路
９　　マイコンの汎用ポート
１０　　デバッグイネーブル（ＤＢＧ＿ＥＮ）レジスタ

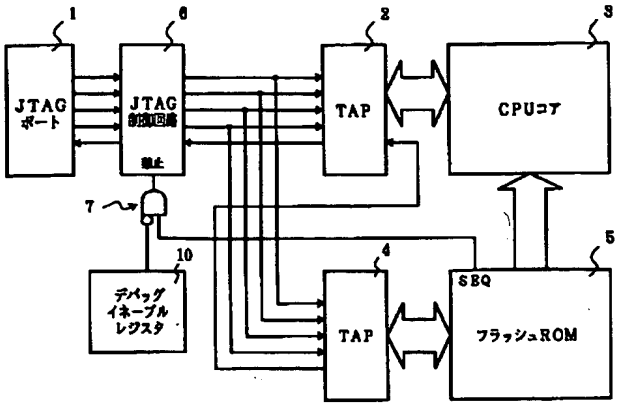
【図１】



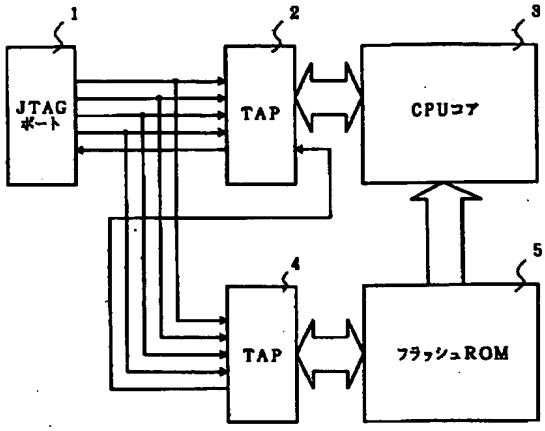
【図２】



【図３】


1
6
2
3
JTAG
ポート
JTAG
制御回路
TAP
CPUコア
7
10
4
5
SEQ
デバッグ
イネーブル
レジスタ
TAP
フラッシュROM

【図４】


1
2
3
JTAG
ポート
TAP
CPUコア
4
5
TAP
フラッシュROM